楕円曲線の等分点の体における相互法則について(代数的整数論)

AUTHOR(S):

山本, 芳彦

CITATION:

山本, 芳彦. 楕円曲線の等分点の体における相互法則について(代数的整数論). 数理解析研究所講究録 1991, 759: 192-197

ISSUE DATE:

1991-06

URL:

http://hdl.handle.net/2433/82184

数理解析研究所講究録
759巻 1991年 192-197

楕円曲線の等分点の体における相互法則について

山本芳彦（大阪大 理）

0. Introduction.

C を有理数体 Q 上に定義される楕円曲線とする．奇素数 l に対して， $K(l) = Q(C[l])$ を C の l-等分点全体 C[l] の座標を Q に添加した体とする．拡大 K(l)/Q は Galois 拡大である． C[l] の生成元 P_1, P_2 を固定することにより $G(l) = Gal(K(l)/Q)$ は $GL_2(Z/lZ)$ の部分群と見ることができる．

C が虚数乗法をもつとき，C の自己準同型環 $E = End(C)$ はある虚 2次体 $k = Q(\sqrt{d})$ の整環(order)となる．このとき，$k\cdot K(l)/k$ は abel拡大であって，この拡大における素イデアルの分解法則は虚数乗法論によって詳しくわかっている．したがって， 拡大 K(l)/Q についてもよくわかっているといえる． しかし C が虚数乗法を持たないとき，すなわち $End(C) = Z$ のときには，G(l) は一般には nonsolvable group となり，K(l)/Q における素点の分解法則についてはあまりよく解っていない． しかし，K(l)/Q は nonsolvable な拡大での素イデアル分解の様子について，不完全ながらも，かなりの様子がわかる数少ない例を提供している．

ここでは， C が虚数乗法をもたない場合にも,素点 p が K(l) で完全分解する条件が，C の reduction modulo p を $\bar{C}$ として，$\bar{C}$ の合同 ζ 関数と 虚 2次体の order の 類方程式(class polynomial) を用いて決定できることを報告する．

1. 合同 ζ 関数による分解法則の表現

N を C の conductor とし，p を $p \nmid lN$ をみたす素数とする． K(l) において p の上にある一つの素点の Frobenius 置換を $\sigma(p)$ とすると，$\sigma(p)$ は G(l) における共役を除いて一意に定まる．$\sigma(p)$ の共役類を決めることが我々の目標である．$C[l] \approx Z/lZ + Z/lZ$ だから，その一組の生成元 P_1, P_2 を定めて，G(l) の表現を ρ_l を，

$$(1\text{-}1) \qquad \begin{bmatrix} P_1{}^{\sigma(p)} \\ P_2{}^{\sigma(p)} \end{bmatrix} = \rho_l(\sigma(p)) \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}, \quad \rho_l(\sigma(p)) \in GL_2(Z/lZ)$$

によって定義すると，ρ_l は単射である． ρ_l により $G(l) \subset GL_2(Z/lZ)$ と考える．

C の reduction modulo p により得られる曲線を $\bar{C}$ とすると， $\bar{C}$ は有限体 F_p 上に定義される楕円曲線となる． そのとき，P_1, P_2 mod p は well-defined でそれを $\bar{P}_1, \bar{P}_2$ とかくと，π を F_p 上の Frobrnius-map として，(1-1) より

$$(1\text{-}2) \qquad \begin{bmatrix} \pi(\bar{P}_1) \\ \pi(\bar{P}_2) \end{bmatrix} = \sigma(p) \begin{bmatrix} \bar{P}_1 \\ \bar{P}_2 \end{bmatrix}$$

が成り立つ． $\bar{C}$ の F_p -有理点 $\bar{C}(F_p)$ の個数を N_p として，$a_p = 1 + p - N_p$ とおくとき， $\sigma(p)$ の固有多項式 $f_p(t)$ が

$$f_p(t) \equiv t^2 - a_p t + p \pmod{l}$$

で与えられる． 右辺の多項式の判別式を $d_p = a_p{}^2 - 4p$ とおく．

$l \nmid d_p$ ならば，$f_p(t)$ は mod l で重根をもたないので $\sigma(p)$ の共役類は一意的に定まる．したがって，このばあいには分解の様子がわかったといえる:

$$\left(\frac{d_p}{l}\right) = 1 \Rightarrow \sigma(p) \sim \begin{bmatrix} b & 0 \\ 0 & b' \end{bmatrix}, \qquad \mathrm{ord}(\sigma) \mid l-1$$

$$\left(\frac{d_p}{l}\right) = -1 \Rightarrow \sigma(p) \sim \begin{bmatrix} 0 & p \\ -1 & a_p \end{bmatrix}, \quad \mathrm{ord}(\sigma) \mid l^2-1, \ \mathrm{ord}(\sigma) \nmid l-1.$$

$l \mid d_p$ のときには，$f_p(t)$ の重根を b とすると，

$$\sigma(p) \sim \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \quad \text{または} \quad \sigma(p) \sim \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix}$$

のいづれかであるが，この決定が難しい．$\sigma(p)$ の位数は，前者の場合には ord(σ) は l-1 の約数だが，後者の場合には ord(σ) は l で割り切れる．この区別をつけたい．次の結果が知られている．

定理(志村 [Sh])

$l \| d_p$ ならば $\sigma(p) \sim \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix}$.

この結果，$l^2 \mid d_p$ のときのみが問題として残っているのだが，その中には最も重要な問題， p が完全分解する，すなわち， $\sigma(p) = 1$ であるための条件を求めることが含まれている． 実際，

$$\sigma(p) = 1 \Rightarrow a_p \equiv 2 \pmod{l} \quad \text{かつ} \quad l^2 \mid d_p$$

(このとき $p \equiv 1 \pmod{l}$).

逆に，

$$a_p \equiv 2 \pmod{l} \text{ かつ } l^2 \mid d_p$$

$$\Rightarrow \sigma(p) = 1 \quad \text{または} \quad \sigma(p) \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

このとき $l^2 \mid N_p$ である． $\bar{C}$ の l-分点 $\bar{C}[l]$ を用いると，

$$\sigma(p) = 1 \quad \Leftrightarrow \quad \bar{C}[l] \subset \bar{C}(F_p)$$

$$\sigma(p) \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \Leftrightarrow \quad \bar{C} \text{ の } F_p\text{-有理点の l-part は cyclic .}$$

次節以降では，$\bar{C}[l]$ 全体が F_p-有理点 になる条件を $\bar{C}$ の自己準同型環 $E_p = \mathrm{End}(\bar{C})$ とそこにおける類体論(ring class field theory)を用いて調べることを目標とする．

2. Class polynomial による E_p の決定

$\bar{C}$ の自己準同型環を $E_p = \mathrm{End}(\bar{C})$ とすると，E_p はある 4元数体または虚 2次体の整環(order)になる．前者の場合に p は supersingular であるといい,後者の場合には p は ordinary であるという． p が supersingular であるためには $a_p \equiv 0 \pmod{p}$ であることが必要かつ十分である．このとき，Frobenius map $\pi: x \to x^p$ は E_p の元で

$$\pi^2 - a_p \pi + p = 0, \qquad d_p = a_p^2 - 4 < 0$$

をみたす．ここで，$1 - a_p + p = N_p = \#\bar{C}(F_p)$.

以後，$p \nmid lN_p$ かつ $l \mid d_p$ とする．このとき，$p \nmid a_p$ となり，p は ordinary prime である． したがって， E_p は 虚 2次体 $k = Q(\sqrt{d_p})$ のある order である，E_p の判別式を d とする．2次体 k の整数環を O，判別式を D とすると

$$O \supset E_p \supset Z[\pi], \quad d = c^2 D, \quad d_p = c_p{}^2 d$$

(c, c_p は正整数) となる． p は ordinary であることより，p は E_p で完全分解して $p = (\pi)(\bar{\pi})$ と 2つの素イデアル積となる．$j(E_p)$ を E_p に対する楕円 modular関数 j の値とすると，$K = k(j(E_p))$ は E_p の環類体で，次が成り立つ．

$$[K : k] = h(E_p) = E_p \text{ の類数}.$$

さらに， 素イデアル (π) は E_p で単項だから K で 完全分解する．(π) の上にある K の 1次の素イデアル Π で

$$j(E_p) \bmod \Pi = jc \ (= jc \bmod p)$$

をみたすものをとる． 虚数乗法論より，K 上定義される楕円曲線 C_1 で次の 2条件をみたすものが存在することがわかる:

(i) $End(C_1) \approx E_p$

(ii) $C_1 \bmod \Pi \approx \bar{C}$ over F_p

$(\Rightarrow jc_1 \bmod \Pi = jc \bmod p = jc)$.

一般に，負の判別式 d をもつ虚 2次体の order $O = O_d$ において，その類数を $h = h(d)$ とし， $I_1, \ldots, I_h$ をイデアル類の代表とするとき，

$$P_d(X) = (X - j(I_1)) \cdots (X - j(I_h))$$

は Z-係数の monicな既約多項式である．$P_d(X)$ を O_d の類多項式という．

例． $P_{-3}(X) = X$

$P_{-4}(X) = X - 1728$

$P_{-15}(X) = X^2 + 191025X - 121287375$

$P_d(X)$ は $k_d = Q(\sqrt{d}\,)$ 上でも既約で，$P_d(X)$ の k_d 上の最小分解体 K_d は O_d の環類体を与える．α を O_d の元で $N\alpha = p$ かつ $\alpha \neq \bar{\alpha}$ なるものとすると，(α) は O_d の素イデアルで K_d において完全分解する．(α) の上にある K_d の素イデアルの 1つを Π とするとき，

$$\{j(I_1), \ldots, j(I_h)\} \xrightarrow{\bmod \Pi} \{j \in F_p : P_d(j) = 0\} \subset F_p$$

は単射である．

これより次がわかる．もとの C にもどって，C の j-invariant を $j_c \in Q$とするとき

$$E_p = O_d \quad \Leftrightarrow \quad d_p = c_p^2\, d \text{ かつ } P_d(j_c) \equiv 0 \pmod p$$

例

$C: Y^2 + Y = X^3 - X^2$　　$\Delta = -11$,　$j = -2^{12}11^{-1}$

$p=101$　$a_p = 2$　$N_p = 100$　$d_p = -400 = 10^2(-4)$

$j \equiv -51 \pmod p$

$c_p=10$　$P_{-4}(X) \equiv X + 90 \pmod p$

$c_p=5$　$P_{-16}(X) \equiv X + 51 \pmod p$

$c_p=2$　$P_{-100}(X) \equiv (X + 59)(X + 32) \pmod p$

$c_p=1$　$P_{-400}(X) \equiv (X + 97)(X + 64)(X + 24)(X + 7) \pmod p$

よって　$d = -16$,　$E_p = Z(\sqrt{-4})$.

3. $\sigma(p)$ の決定

今までの議論により，有理数体上定義された楕円曲線 C において，p を $p \nmid lN_p$ である ordinary prime として，$\bar{C}$ を C の reduction mod p，$E_p = \mathrm{End}(\bar{C})$，$E_p$ の判別式を d とする．$\bar{C}$ の Frobenius map を π とし，E_p の 環類体 K における (π) の素因子のひとつを Π とするとき，K 上に定義される楕円曲線 C_1 で

$$\mathrm{End}(C_1) \approx E_p\,, \qquad C_1 \bmod \Pi \approx \bar{C}$$

なるものが存在する．K(l) を E_p の conductor l の 環類体とすると，K(l) は K に C_1 の l 分点 $C_1[l]$ の x-座標成分(Weber function の

値)全体 $x(C_1[l])$ を添加することにより得られる．したがって，次が成り立つ: $d < -4$ のとき

$$\pi \equiv \pm 1 \pmod{lE_p}$$
$$\Leftrightarrow \quad (\pi) \text{ は } K(l) \text{ で完全分解する．}$$
$$\Leftrightarrow \quad \pi \text{ は } x(C_1[l] \bmod \Pi) = x(\bar{C}[l]) \text{ に trivial に作用する．}$$
$$\Leftrightarrow \quad \sigma(p) = \pm 1 \ .$$

ここで $\pi = \dfrac{a_p + \sqrt{d_p}}{2}$ ， $l \mid d_p = c_p^2 d$ より，

$l \nmid a_p$ の仮定の下で，

$$l \mid c_p \ \Rightarrow \ \pi \equiv a_p/2 \pmod{lE_p}$$
$$\Rightarrow \ (E_p/lE_p)^\times \text{ で } \mathrm{ord}(\pi) \mid l-1$$
$$\Rightarrow \ \mathrm{ord}(\sigma(p)) \mid l-1 \ .$$

$$l \nmid c_p \ \Rightarrow \ (E_p/lE_p)^\times \text{ で } l \mid \mathrm{ord}(\pi)$$
$$\Rightarrow \ l \mid \mathrm{ord}(\sigma(p)) \ .$$

定理

C の j-invariant を jc とする．$l \mid d_p$ のとき，

(i) $d_p = c_p^2 d$, $P_d(jc) \equiv 0 \pmod{p}$ をみたす虚 2次の order の判別式 d が唯一つ存在する．このとき $E_p = O_d$ が成立する．

(ii) $\sigma(p) \sim \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \Leftrightarrow l \mid c_p$.

References

[Sh] Shimura, G.: A reciprocity law in non-solvable extensions, J. Reine Angew. Math., 221(1966), 209-220.